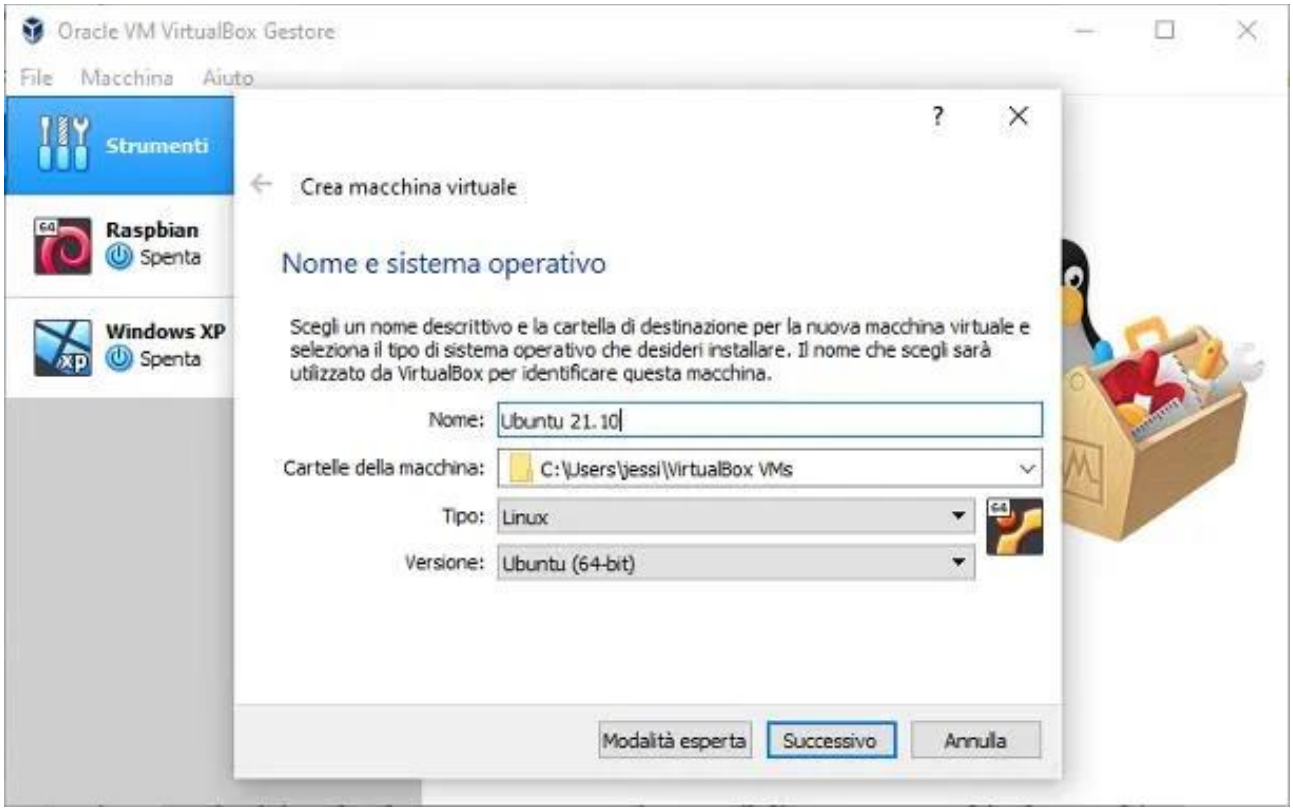
ANALISI DINAMICA BASICA

Per svolgere questo esercizio di analisi dinamica su un malware utilizzando Process Monitor (procmon), è necessario seguire una serie di passi per identificare le azioni del malware sul file system, sui processi e thread, e le modifiche del registro di sistema. Di seguito è riportata una guida dettagliata per completare ciascuna delle richieste:

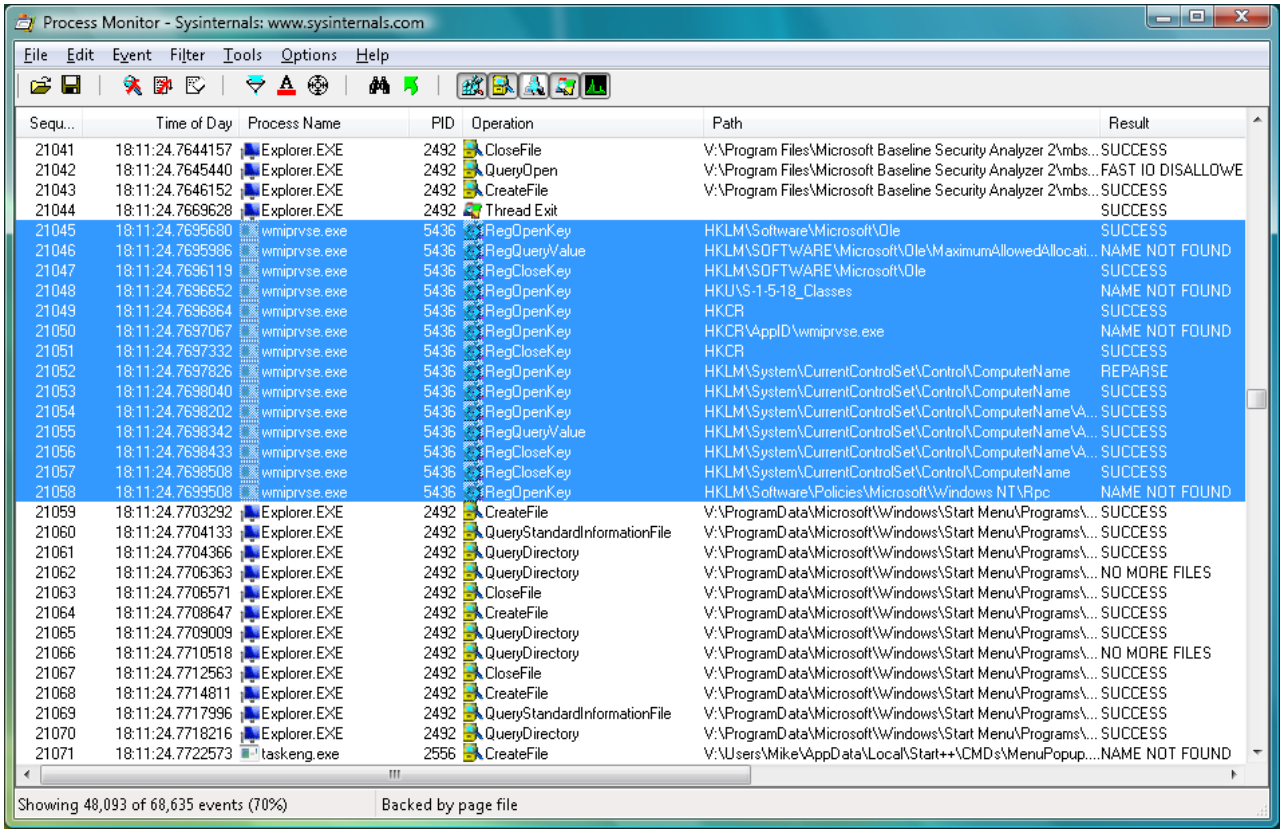
Passi Preliminari:

1. **Creare un'istantanea della macchina virtuale:**
    - Aprire VirtualBox.
    - Selezionare la macchina virtuale Windows XP.
    - Fare clic su "Istantanee" e poi su "Prendi istantanea".
    - Assegnare un nome all'istantanea e fare clic su "OK".
    - In alternativa, è possibile clonare la macchina virtuale.



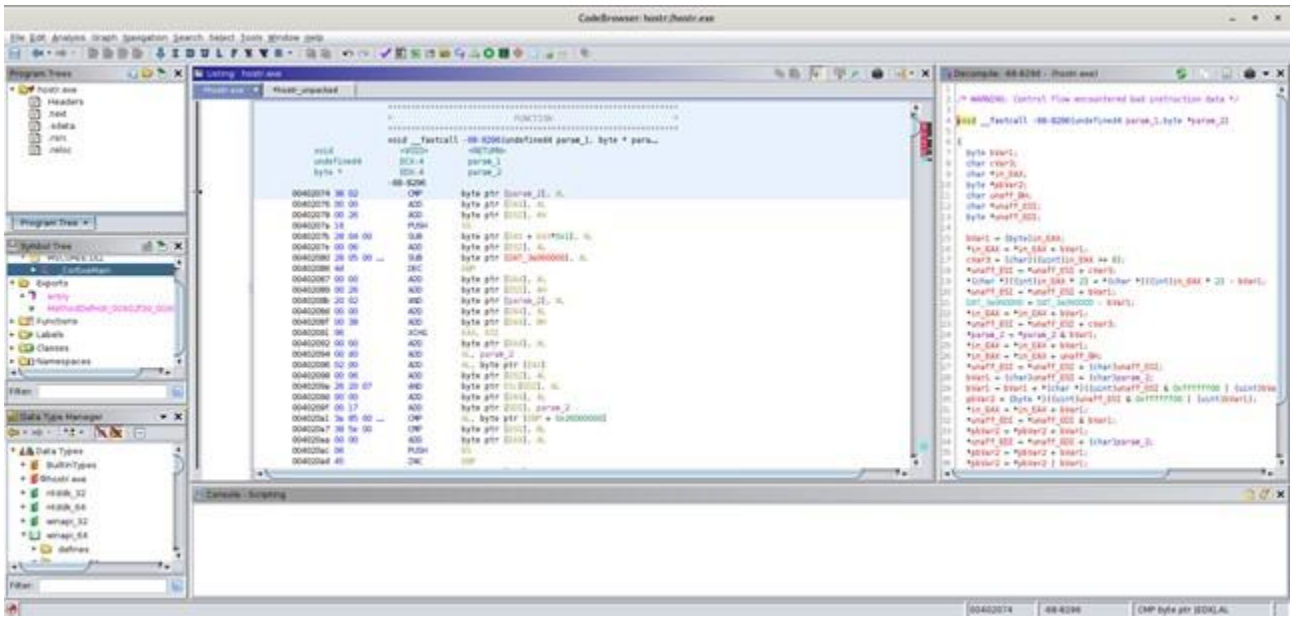
1. Identificare Azioni del Malware sul File System:

- **Avviare Process Monitor:**
  - Avviare la macchina virtuale Windows XP.
  - Eseguire Process Monitor (procmon.exe).
  - Configurare i filtri per visualizzare solo le operazioni rilevanti:
    - Filtrare per operazioni di file system selezionando `Operation` e scegliendo `CreateFile`, `WriteFile`, `ReadFile`, `DeleteFile`, ecc.
    - Filtrare per il path noto dove si trova l'eseguibile del malware (es., C:\path\to\malware.exe).



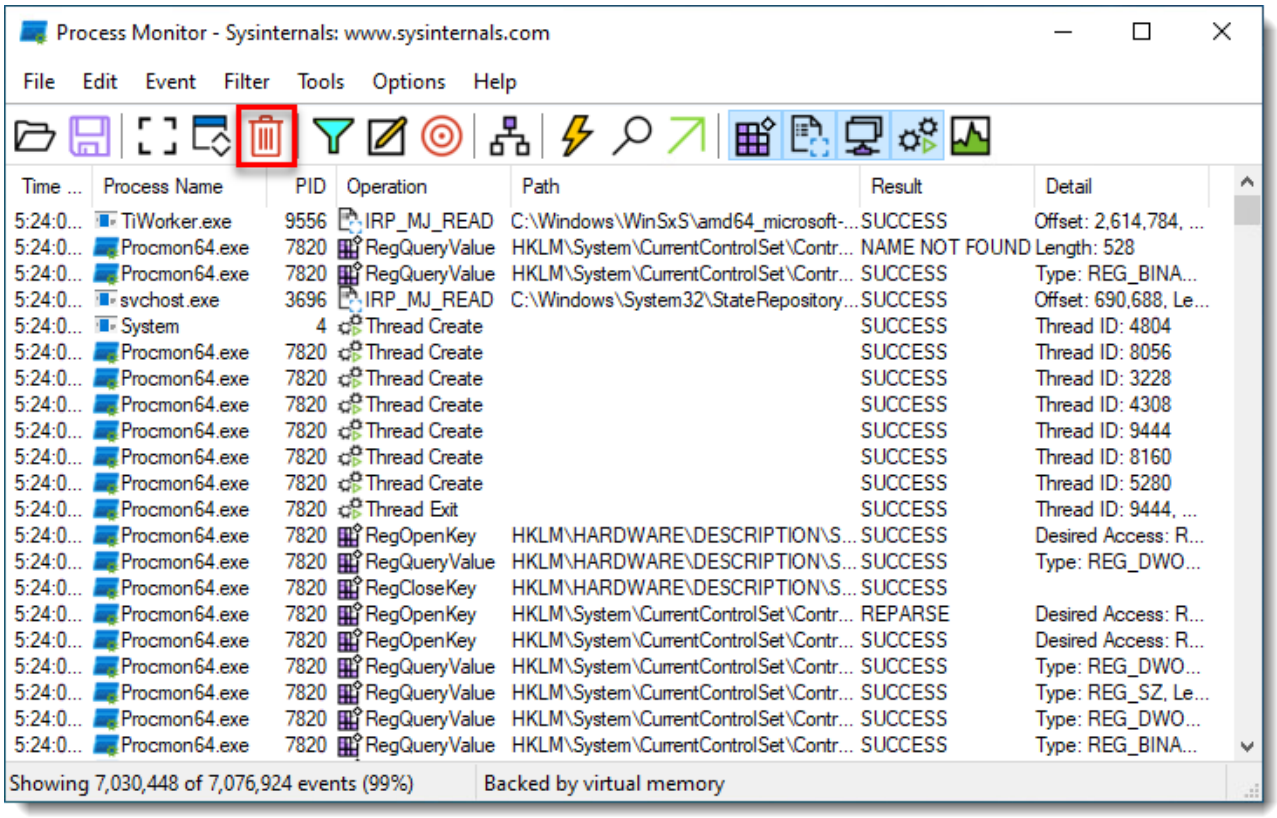
Sequ...	Time of Day	Process Name	PID	Operation	Path	Result
21041	18:11:24.7644157	Explorer.EXE	2492	CloseFile	V:\Program Files\Microsoft Baseline Security Analyzer 2\mbs...	SUCCESS
21042	18:11:24.7645440	Explorer.EXE	2492	QueryOpen	V:\Program Files\Microsoft Baseline Security Analyzer 2\mbs...	FAST IO DISALLOWE
21043	18:11:24.7646152	Explorer.EXE	2492	CreateFile	V:\Program Files\Microsoft Baseline Security Analyzer 2\mbs...	SUCCESS
21044	18:11:24.7669628	Explorer.EXE	2492	Thread Exit		SUCCESS
21045	18:11:24.7695680	wmiprvse.exe	5436	RegOpenKey	HKLM\Software\Microsoft\Ole	SUCCESS
21046	18:11:24.7695986	wmiprvse.exe	5436	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\MaximumAllowedAllocati...	NAME NOT FOUND
21047	18:11:24.7696119	wmiprvse.exe	5436	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole	SUCCESS
21048	18:11:24.7696652	wmiprvse.exe	5436	RegOpenKey	HKU\S-1-5-18_Classes	NAME NOT FOUND
21049	18:11:24.7696864	wmiprvse.exe	5436	RegOpenKey	HKCR	SUCCESS
21050	18:11:24.7697067	wmiprvse.exe	5436	RegOpenKey	HKCR\AppID\wmiprvse.exe	NAME NOT FOUND
21051	18:11:24.7697332	wmiprvse.exe	5436	RegCloseKey	HKCR	SUCCESS
21052	18:11:24.7697826	wmiprvse.exe	5436	RegOpenKey	HKLM\System\CurrentControlSet\Control\ComputerName	REPARSE
21053	18:11:24.7698040	wmiprvse.exe	5436	RegOpenKey	HKLM\System\CurrentControlSet\Control\ComputerName	SUCCESS
21054	18:11:24.7698202	wmiprvse.exe	5436	RegOpenKey	HKLM\System\CurrentControlSet\Control\ComputerName\A...	SUCCESS
21055	18:11:24.7698342	wmiprvse.exe	5436	RegQueryValue	HKLM\System\CurrentControlSet\Control\ComputerName\A...	SUCCESS
21056	18:11:24.7698433	wmiprvse.exe	5436	RegCloseKey	HKLM\System\CurrentControlSet\Control\ComputerName\A...	SUCCESS
21057	18:11:24.7698508	wmiprvse.exe	5436	RegCloseKey	HKLM\System\CurrentControlSet\Control\ComputerName	SUCCESS
21058	18:11:24.7699508	wmiprvse.exe	5436	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows NT\Rpc	NAME NOT FOUND
21059	18:11:24.7703292	Explorer.EXE	2492	CreateFile	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	SUCCESS
21060	18:11:24.7704133	Explorer.EXE	2492	QueryStandardInformationFile	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	SUCCESS
21061	18:11:24.7704366	Explorer.EXE	2492	QueryDirectory	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	SUCCESS
21062	18:11:24.7706363	Explorer.EXE	2492	QueryDirectory	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	NO MORE FILES
21063	18:11:24.7706571	Explorer.EXE	2492	CloseFile	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	SUCCESS
21064	18:11:24.7708647	Explorer.EXE	2492	CreateFile	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	SUCCESS
21065	18:11:24.7709009	Explorer.EXE	2492	QueryDirectory	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	SUCCESS
21066	18:11:24.7710518	Explorer.EXE	2492	QueryDirectory	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	NO MORE FILES
21067	18:11:24.7712563	Explorer.EXE	2492	CloseFile	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	SUCCESS
21068	18:11:24.7714811	Explorer.EXE	2492	CreateFile	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	SUCCESS
21069	18:11:24.7717996	Explorer.EXE	2492	QueryStandardInformationFile	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	SUCCESS
21070	18:11:24.7718216	Explorer.EXE	2492	QueryDirectory	V:\ProgramData\Microsoft\Windows\Start Menu\Programs\...	SUCCESS
21071	18:11:24.7722573	taskeng.exe	2556	CreateFile	V:\Users\Mike\AppData\Local\Start++\CMDs\MenuPopup....	NAME NOT FOUND

- **Eseguire l'eseguibile del malware:**
  - Eseguire il malware dal percorso specificato.
- **Monitorare le operazioni:**
  - Osservare le chiamate alla funzione `CreateFile` e altre operazioni di file system.
  - Annotare i percorsi e le operazioni eseguite dal malware.



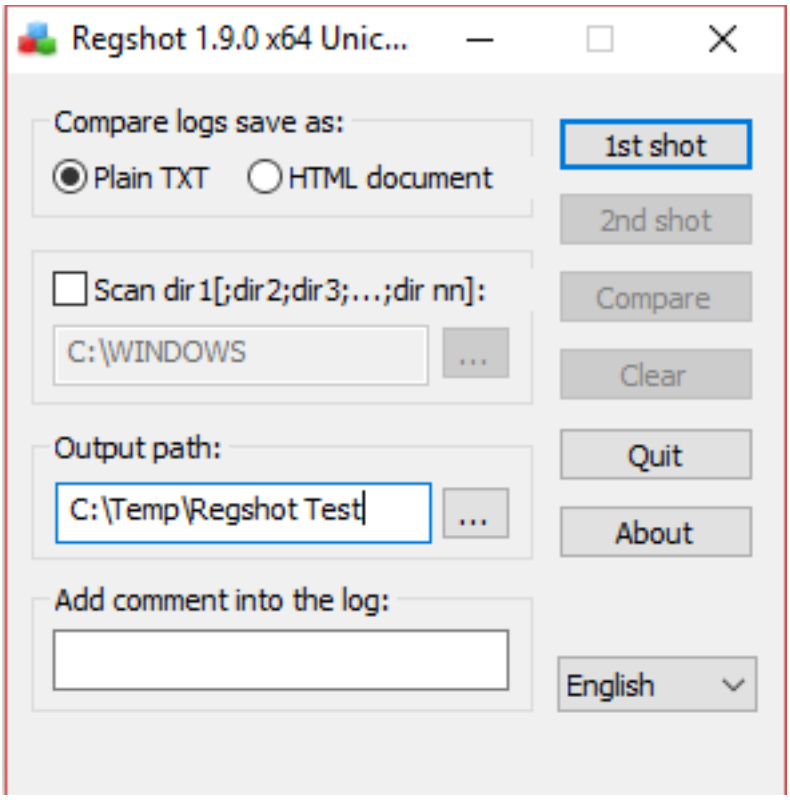
2. Identificare Azioni del Malware su Processi e Thread:

- **Configurare Process Monitor per Processi e Thread:**
  - Filtrare per operazioni di processi e thread selezionando `Operation` e scegliendo `Process Create`, `Process Exit`, `Thread Create`, `Thread Exit`, ecc.
- **Eseguire il malware e monitorare:**
  - Eseguire di nuovo il malware e osservare le nuove operazioni sui processi e thread.
  - Annotare i nuovi processi e thread creati o terminati.



3. Identificare Modifiche al Registro di Sistema:

- **Preparare un confronto del registro:**
  - Prima di eseguire il malware, esportare una copia del registro:
    - Aprire l'Editor del Registro di Sistema (`regedit.exe`).
    - Selezionare `Computer`, fare clic con il tasto destro e scegliere `Esporta`.
    - Salvare il file con un nome appropriato (es., `pre_malware.reg`).
- **Eseguire il malware:**
  - Eseguire il malware come nei passi precedenti.
- **Esportare nuovamente il registro:**
  - Dopo l'esecuzione del malware, esportare di nuovo una copia del registro (es., `post_malware.reg`).
- **Confrontare le differenze:**
  - Utilizzare un tool di comparazione del registro, come `Regshot` o uno strumento simile:
    - Eseguire il confronto tra `pre_malware.reg` e `post_malware.reg`.
    - Annotare le differenze rilevate, in particolare le chiavi create, modificate o eliminate.



Report delle Scoperte:

- **Preparare un report dettagliato:**
  - Elencare le azioni sul file system (CreateFile, WriteFile, etc.), includendo i percorsi specifici.
  - Documentare i processi e i thread creati o modificati.
  - Dettagliare le modifiche del registro con le chiavi e i valori modificati.

Considerazioni Finali:

- **Ripristinare l'istantanea della macchina virtuale:**
  - Utilizzare VirtualBox per ripristinare l'istantanea creata in precedenza, garantendo che il sistema sia pulito per ulteriori analisi o test.